Networking Technology

Outputs

- Definition of structured planning process for telecommunication and information technology networks.
- Suggestions for types of tools to assist in network design and administration.
- Handbook for telecommunication and information technology network planning (will be available in 2003 on ITS programs webpage http://www.its.bldrdoc.gov/home/projects.html)

The Institute has a long history of performing telecommunication planning and assessment studies for other organizations, but the complexity of today's telecommunication and information technology (hereafter "telecom and IT") requirements, and the technology available to satisfy those requirements, create demands for enhanced sophistication in the methodologies and tools used to perform these studies. The Networking Technology project has defined a structured planning process for such studies, examined many tools that can be used in conducting such studies, and identified those tools most likely to provide the greatest benefits. Last year's Technical Progress Report showed the use of these tools in discovering the topology of a network, the loads on segments of the network, and simulating the migration of the topology and loads to a new topology. Efforts in FY 2002 focused on two of the most important aspects of network design and administration: Network Management and Network Security.

Network Management

Network management can be defined as the ability to control the activities required in managing a network from a single point on that network. This point can be at several locations, thus allowing management staff to quickly perform functions from many locations on the network. Good network management can help any organization achieve its goals of availability and performance. Poor network management will not only *not* help an organization reach its goals but may also contribute to the problems which prevent the achievement of those goals.

A logical approach to network management is to break down the management function into its component parts and ensure that each part can be performed efficiently using tools and trained personnel. The International Organization for Standardization (ISO) defines five types of network management functions:

1. *Fault management* refers to detecting, isolating, reporting, diagnosing, and correcting faults on the network. A variety of tools exist to meet these fault management requirements, including monitoring tools, polling tools, alarming tools, report generation tools, and protocol analyzers.

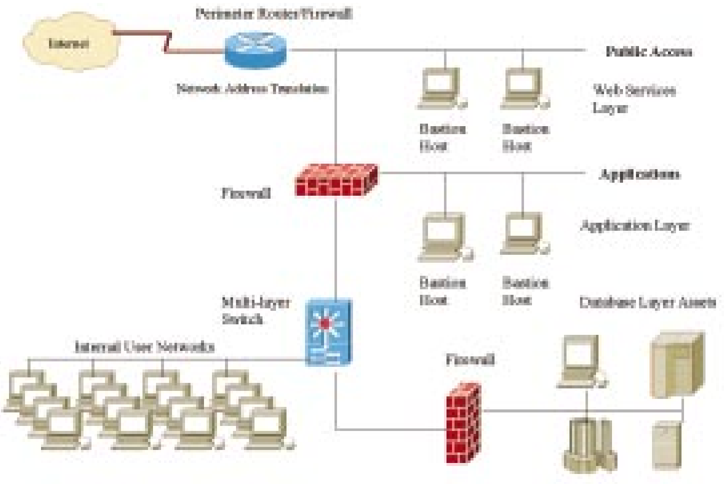
2. *Performance management* is the ability to measure network behavior and effectiveness. This includes protocol performance, application performance, response times across the network, and the reachability of network components. Tools that monitor and measure performance include network analyzers, RMON monitors, and tools that utilize built-in capabilities of many network devices.

3. *Security management* protects network components and interconnections from unauthorized access, unauthorized use, and other damage. This function maintains audit logs, records logins and logouts, and records attempts by users to change their level of authorization. Tools for security management include firewall, intrusion detection systems, perimeter routers, and virtual private networks.

4. *Configuration management* allows the manager to control the configuration of the network and manage the network assets in a logical, systematic, and organized manner. Configuration tools allow the network manager to keep track of operating system configurations and local configurations of devices as well as changes to devices.

5. *Accounting management* allows the administrators to collect statistical information on network usage and load on a component, user, or group level. This facilitates usage-based billing of network customers and can be an aid in detecting abuse of network resources. Another practical reason for accounting management is to track network load levels so that future capacity planning can be undertaken with more confidence in the predicted levels of growth.

Network Security



A layered secure network topology.

Every organization has a mission. In this “information age,” as individuals and organizations use information technology systems to process information and further their mission, security management is critical in protecting each organization’s assets, and thus its mission, from damage. In recent years and especially since September 11, 2001, security has become a major concern of network designers and administrators. The cost of lost data and time, as well as the potential damage to an organization’s image and stability, requires that the network administrator or designer place a very high emphasis on network security. To ensure that a comprehensive, detailed, relevant, and effective security management system is developed, it is important to start by creating a procedure for its creation that covers all aspects of security planning and implementation. This procedure will provide a baseline that organizations can reference when the network security is regularly re-evaluated. A logical approach to security management follows the steps listed below:

1. Define clear principles and practices for securing the IT system.
2. Define an IT security framework for implementing the security management system.
3. Identify overall security requirements.
4. Identify existing assets to be secured.
5. Identify the security risks and consequences of failure of these assets.
6. Analyze security trade-offs and costs for required security level for these assets.
7. Develop a security plan.
8. Develop a security policy.
9. Document procedures and controls for implementing the security plan and policy.
10. Implement the policy through adequate training and resource allocation.
11. Integrate the policy with the organization’s overall security management system.
12. Review and reassess the security management system periodically or as the network or security requirements change.

Security considerations have a major impact on network topology and the experience of the network designer is critical in this effort. When designing a network, the designer must consider trade-offs of cost with the level of performance and security provided. Since this is the case, there are many ways that a network solution and design can be implemented. A basic secure network design assumes that the organization’s assets will be broken down into three layers of access and sensitivity. This configuration is shown in the figure. The three layers are:

Layer 1 - Public access layer. This layer allows public access to those services and data that the security plan permits. The security policy and risk assessment dictate how that access is achieved, who is permitted access, and how the assets are managed. Data and services at this layer have the lowest sensitivity and the lowest level of security.

Layer 2 - Application layer. This layer supports the services in layer 1 without allowing direct access to the services by the requesting user. This protects the application assets from unauthorized access or modification. Services in layer 1 are permitted to access the applications in layer 2 via a bastion host and firewall. Data and services at this layer have moderate sensitivity and a moderate level of security.

Layer 3 - Database layer. This layer supports database requirements of applications operating in layer 2. These assets are considered very sensitive and must be given the greatest level of security. Direct access to this layer by users is prohibited or at least severely restricted.

For more information, contact:
Robert O. DeBolt
(303) 497-5324
e-mail rdebolt@its.bldrdoc.gov